

Obsah

Předmluva	v
1 Numerické výpočty a jejich chyby	1
1.1 Numerické chyby a jejich charakteristika	2
1.2 Chyba při výpočtu hodnot funkcí	4
1.3 Inverze úlohy určení chyby při výpočtu hodnot funkcí	4
1.4 Podmíněnost úloh	6
1.5 Aritmetika s pohyblivou řádovou čárkou	6
1.5.1 IEEE standardní aritmetiky	7
1.5.2 Přesnost zobrazení reálných čísel v IEEE aritmetice	9
1.6 Zaokrouhlovací chyby v aritmetice s konečnou přesností	9
2 Řešení soustav lineárních algebraických rovnic	13
2.1 Úvod — Soustavy lineárních rovnic	13
2.2 Gaussova eliminační metoda	14
2.3 Jacobiho iterační metoda	18
2.4 Gauss-Seidlova iterační metoda	19
2.5 Metoda LU-rozkladu	20
2.6 Metoda LU-rozkladu a Gaussova eliminační metoda	21
3 Řešení soustav nelineárních rovnic	23

3.1	Iterační metoda	23
3.2	Newtonova metoda	26
3.3	Gradientní metoda	28
4	Metoda nejmenších čtverců	33
4.1	Aproximace pomocí lineární funkce	33
4.2	Skalární součin a norma vektorů při daných váhách	35
4.3	Existence minima kvadratické odchylky v prostoru	36
5	Aritmetika kódu zbytkových tříd	39
5.1	Jedno-modulová aritmetika kódu zbytkových tříd	39
5.1.1	Aplikace teorie	43
5.2	Největší společný dělitel	44
5.3	Euklidův algoritmus	46
5.4	Základní věta aritmetiky	47
5.5	Vlastnosti prvočísel	51
5.6	Umocňování v modulární aritmetice	57
5.7	Více-modulová aritmetika kódu zbytkových tříd	58
5.8	Aritmetika v \mathbb{Z}_β	60
5.9	Převod z kódu zbytkových tříd do celých čísel	62
5.9.1	Výpočet d_i s použitím reziduální aritmetiky	64
5.10	Přesný výpočet SLR v modulární aritmetice	68
5.10.1	Celočíselné vstupní hodnoty	69
6	Reziduální aritmetika v kryptografii	75
6.1	Znakové šifry	75
6.2	Blokové šifry	80
6.3	Exponenciální šifry	84

6.4	Kryptografie veřejného klíče	88
6.5	Kryptografie eliptických křivek	92
6.5.1	Eliptická křivka nad tělesem $GF(p)$	94
6.5.2	Šifrování s ECC	96

Předkládaný učební text je určen především pro studenty numerické matematiky, programování při jeho studiu. ANM vznikl z větší části podle pří vědeckém výzkumu.

Text je rozdělen do dvou částí. První část je věnována základům numerické matematiky a lineárním a nelineárním vybraným problémům. Druhá část je věnována řešení soustav rovnic a k dalšímu smysluplnému využití. Text je doplněn o mnoho příkladů a je nadobudými příklady, které vedou k získání nových poznatků. V podkapitole 5.10 je uvedeno, jak se lze obrátit na autora.

Druhá část tohoto učebního textu je věnována řešení soustav rovnic a k dalšímu smysluplnému využití. Text je doplněn o mnoho příkladů a je nadobudými příklady, které vedou k získání nových poznatků. V podkapitole 5.10 je uvedeno, jak se lze obrátit na autora.

První část předkládaného učebního textu je věnována řešení soustav rovnic a k dalšímu smysluplnému využití. Text je doplněn o mnoho příkladů a je nadobudými příklady, které vedou k získání nových poznatků. V podkapitole 5.10 je uvedeno, jak se lze obrátit na autora.

Je mou milou povinností poděkovat kolegům z ústavu za jejich rady a opravy textu.

Brno, říjen 2003